(5) Die in Absatz 1 genannten Finanzunternehmen stellen sicher, dass ihr vereinfachter IKT-Risikomanagementrahmen im Einklang mit dem Revisionsplan des betreffenden Finanzunternehmens einer internen Revision durch Revisoren unterzogen wird. Die Revisoren müssen über ausreichendes Wissen und ausreichende Fähigkeiten und Fachkenntnisse im Bereich IKT-Risiken verfügen und unabhängig sein. Häufigkeit und Schwerpunkt der IKT-Revisionen müssen den IKT-Risiken des Finanzunternehmens angemessen sein.

(6) Auf der Grundlage der Ergebnisse der in Absatz 5 genannten Revision stellen die in Absatz 1 genannten Finanzunternehmen die rechtzeitige Überprüfung und Auswertung kritischer Erkenntnisse der IKT-Revision sicher.

Artikel 29

Informationssicherheitsleitlinien und -maßnahmen

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen erarbeiten, dokumentieren und implementieren im Zusammenhang mit dem vereinfachten IKT-Risikomanagementrahmen eine Informationssicherheitsleitlinie. Diese Informationssicherheitsleitlinie enthält die übergeordneten Grundsätze und Regeln zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Daten und der von diesen Finanzunternehmen erbrachten Dienstleistungen.

(2) Auf der Grundlage ihrer in Absatz 1 genannten Informationssicherheitsleitlinie legen die in Absatz 1 genannten Finanzunternehmen IKT-Sicherheitsmaßnahmen zur Minderung ihres IKT-Risikos fest und setzen diese um, einschließlich Risikominderungsmaßnahmen, die von IKT-Drittdienstleistern umgesetzt werden.

Die IKT-Sicherheitsmaßnahmen müssen alle in den Artikeln 30 bis 38 genannten Maßnahmen umfassen.

Artikel 30

Klassifizierung von Informations- und IKT-Assets

(1) Im Zuge des in Artikel 16 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten vereinfachten IKT-Risikomanagementrahmens ermitteln, klassifizieren und dokumentieren die in Absatz 1 jenes Artikels genannten Finanzunternehmen alle kritischen oder wichtigen Funktionen, die Informations- und IKT-Assets, die diese Funktionen unterstützen, und deren wechselseitige Abhängigkeiten. Die Finanzunternehmen überprüfen diese Ermittlung und Klassifizierung bei Bedarf.

(2) Die in Absatz 1 genannten Finanzunternehmen ermitteln alle kritischen oder wichtigen Funktionen, die von IKT-Drittdienstleistern unterstützt werden.

Artikel 31

IKT-Risikomanagement

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen nehmen in ihren vereinfachten IKT-Risikomanagementrahmen alles Folgende auf:

a) eine Bestimmung der Risikotoleranzschwellen für das IKT-Risiko im Einklang mit der Risikobereitschaft des Finanzunternehmens;

b) die Ermittlung und Bewertung der IKT-Risiken, denen das Finanzunternehmen ausgesetzt ist;

c) die Festlegung von Abmilderungsstrategien zumindest für die IKT-Risiken, die jenseits der Risikotoleranzschwellen des Finanzunternehmens liegen;

d) die Überwachung der Wirksamkeit der unter Buchstabe c genannten Abmilderungsstrategien;

e) die Ermittlung und Bewertung etwaiger IKT- und Informationssicherheitsrisiken, die sich aus größeren Veränderungen des IKT-Systems oder der IKT-Dienstleistungen, -Prozesse oder -Verfahren sowie aus den Testergebnissen in Bezug auf die IKT-Sicherheit und nach schwerwiegenden IKT-bezogenen Vorfällen ergeben.

(2) Die in Absatz 1 genannten Finanzunternehmen führen die IKT-Risikobewertung dem IKT-Risikoprofil der Finanzunternehmen entsprechend regelmäßig durch und dokumentieren sie.

(3) Die in Absatz 1 genannten Finanzunternehmen überwachen fortlaufend Bedrohungen und Schwachstellen, die für ihre kritischen oder wichtigen Funktionen sowie für Informations- und IKT-Assets relevant sind und überprüfen regelmäßig die Risikoszenarien, die sich auf diese kritischen oder wichtigen Funktionen auswirken.

(4) Die in Absatz 1 genannten Finanzunternehmen legen Alarmschwellen und -kriterien für die Auslösung und Einleitung von Reaktionsprozessen bei IKT-bezogenen Vorfällen fest.

Artikel 32

Physische Sicherheit und Sicherheit vor Umweltereignissen

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen ermitteln und implementieren physische Sicherheitsmaßnahmen, die ausgehend von der Bedrohungslage und entsprechend der in Artikel 30 Absatz 1 der vorliegenden Verordnung genannten Klassifizierung sowie auf Basis des Gesamtrisikoprofils der IKT-Assets und der zugänglichen Informationsassets konzipiert werden.

(2) Die in Absatz 1 genannten Maßnahmen schützen die Räumlichkeiten der Finanzunternehmen und, sofern anwendbar, die Rechenzentren von Finanzunternehmen, in denen IKT- und Informationsassets untergebracht sind, vor unbefugtem Zugriff, Angriffen und Unfällen sowie vor Umweltbedrohungen und -gefahren.

(3) Der Schutz vor Umweltbedrohungen und -gefahren muss der Bedeutung der betreffenden Räumlichkeiten und, sofern anwendbar, der Rechenzentren und der Kritikalität der dort untergebrachten Geschäftstätigkeiten oder IKT-Systeme angemessen sein.

KAPITEL II

Weitere Elemente der Systeme, Protokolle und Tools zur Minimierung der Auswirkungen von IKT-Risiken

Artikel 33

Zugangskontrolle

Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen erarbeiten, dokumentieren und implementieren Verfahren für die Kontrolle des logischen und physischen Zugangs und setzen diese Verfahren durch, überwachen sie und überprüfen sie regelmäßig. Diese Verfahren umfassen die folgenden Elemente der Kontrolle des logischen und physischen Zugangs:

a) Verwaltung der Rechte auf Zugang zu Informationsassets, IKT-Assets und den durch sie unterstützten Funktionen sowie zu kritischen Betriebsstandorten des Finanzunternehmens nach dem Grundsatz „Kenntnis nur, wenn nötig“ („Need-to-know“), nach dem Grundsatz der Nutzungsnotwendigkeit („Need-to-use“) und nach dem Grundsatz der minimalen Berechtigung („Least privileges“), auch für den Fern- und Notfallzugang;

b) Zurechenbarkeit der Nutzer, die sicherstellt, dass die Nutzer, die Handlungen in den IKT-Systemen vorgenommen haben, identifiziert werden können;

c) Kontoverwaltungsverfahren für die Gewährung, Veränderung oder Entziehung von Zugangsrechten für Nutzerkonten und generische Konten, insbesondere auch für generische Administratorkonten;

d) Authentifizierungsmethoden, die der in Artikel 30 Absatz 1 genannten Klassifizierung und dem Gesamtrisikoprofil der IKT-Assets angemessen sind und auf führenden Praktiken beruhen;

e) regelmäßige Überprüfung der Zugangsrechte und Entziehung nicht mehr benötigter Zugangsrechte.

Für die Zwecke von Buchstabe c weist das Finanzunternehmen den privilegierten Zugang, den Notfallzugang und den Administratorzugang bei allen IKT-Systemen nach dem Grundsatz der Nutzungsnotwendigkeit oder ad hoc zu und protokolliert den Zugang nach Maßgabe von Artikel 34 Absatz 1 Buchstabe f in einer Log-Datei.

Für die Zwecke von Buchstabe d wenden die Finanzunternehmen starke Authentifizierungsmethoden an, die sich auf führende Praktiken für den Fernzugriff auf das Netz der Finanzunternehmen, für den privilegierten Zugang und für den Zugang zu IKT-Assets zur Unterstützung kritischer oder wichtiger Funktionen stützen, die öffentlich verfügbar sind.

Artikel 34

IKT-Betriebssicherheit

Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen müssen im Rahmen ihrer Systeme, Protokolle und Tools sowie bei allen IKT-Assets

a) den Lebenszyklus aller IKT-Assets überwachen und managen;

b) überwachen, ob die IKT-Assets von IKT-Drittdienstleistern der Finanzunternehmen unterstützt werden, sofern anwendbar;

c) die Kapazitätsanforderungen ihrer IKT-Assets und Maßnahmen ermitteln, um die Verfügbarkeit und Effizienz der IKT-Systeme zu wahren und zu verbessern und IKT-Kapazitätsengpässen vorzubeugen, bevor sie auftreten;

d) eine automatisierte Schwachstellensuche sowie Bewertungen der IKT-Assets durchführen, die der in Artikel 30 Absatz 1 genannten Klassifizierung und dem Gesamtrisikoprofil des betreffenden IKT-Assets angemessen sind, und Patches zur Behebung ermittelter Schwachstellen installieren;

e) die mit veralteten oder nicht unterstützten IKT-Assets oder mit IKT-Altsystemen verbundenen Risiken managen;

f) Vorfälle im Zusammenhang mit der logischen und physischen Zugangskontrolle, dem IKT-Betrieb, einschließlich System- und Netzwerkverkehr, sowie dem IKT-Änderungsmanagement protokollieren;

g) Maßnahmen ermitteln und umsetzen, um Informationen über anomale Aktivitäten und anomales Verhalten bei kritischen oder wichtigen IKT-Vorgängen zu überwachen und zu analysieren;

h) Maßnahmen zur Überwachung relevanter und aktueller Informationen über Cyberbedrohungen umsetzen;

i) Maßnahmen zur Erkennung etwaiger Informationslecks, Schadcodes und anderer Sicherheitsbedrohungen sowie öffentlich bekannter Schwachstellen in Software und Hardware umsetzen und die Verfügbarkeit entsprechender neuer Sicherheitsupdates prüfen.

Für die Zwecke von Buchstabe f stimmen die Finanzunternehmen den Detaillierungsgrad der Protokolle auf deren Zweck und auf die Nutzung des IKT-Assets ab, der diese Protokolle produziert.

Artikel 35

Daten-, System- und Netzwerksicherheit

Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen entwickeln und implementieren im Rahmen ihrer Systeme, Protokolle und Tools Schutzvorrichtungen, die die Sicherheit der Netzwerke gegen Eindringen und den Missbrauch von Daten gewährleisten und die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten wahren. Insbesondere tragen die Finanzunternehmen unter Berücksichtigung der in Artikel 30 Absatz 1 genannten Klassifizierung für alles Folgende Sorge:

a) Ermittlung und Umsetzung von Maßnahmen zum Schutz von Daten, die gerade verwendet oder übermittelt werden, sowie von Daten, die gespeichert sind;

b) Ermittlung und Umsetzung von Sicherheitsmaßnahmen für die Nutzung von Software, Datenträgern, Systemen und Endgeräten, die Daten des Finanzunternehmens übertragen und speichern;

c) Ermittlung und Umsetzung von Maßnahmen zur Verhinderung und Aufdeckung unbefugter Verbindungen mit dem Netz des Finanzunternehmens und zur Sicherung des Netzverkehrs zwischen den internen Netzwerken des Finanzunternehmens und dem Internet und anderen externen Verbindungen;

d) Ermittlung und Umsetzung von Maßnahmen zur Gewährleistung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten bei Netzwerkübertragungen;

e) ein Verfahren zur sicheren Löschung von Daten in den Räumlichkeiten oder von extern gespeicherten Daten, die das Finanzunternehmen nicht mehr erheben oder speichern muss;

f) ein Verfahren zur sicheren Entsorgung oder Außerbetriebnahme von Datenspeichern in den Räumlichkeiten oder von extern gelagerten Datenspeichern, die vertrauliche Informationen enthalten;

g) Ermittlung und Umsetzung von Maßnahmen, mit denen sichergestellt wird, dass Telearbeit und die Nutzung privater Endgeräte die Fähigkeit des Finanzunternehmens, seine kritischen Tätigkeiten angemessen, rechtzeitig und sicher auszuführen, nicht beeinträchtigen.

Artikel 36

IKT-Sicherheitstests

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen erstellen und implementieren einen Plan für IKT-Sicherheitstests, um die Wirksamkeit ihrer gemäß den Artikeln 33, 34 und 35 sowie 37 und 38 der vorliegenden Verordnung entwickelten IKT-Sicherheitsmaßnahmen zu bestätigen. Die Finanzunternehmen stellen sicher, dass in diesem Plan Bedrohungen und Schwachstellen berücksichtigt werden, die im Zuge des in Artikel 31 genannten vereinfachten IKT-Risikomanagementrahmens ermittelt wurden.

(2) Die in Absatz 1 genannten Finanzunternehmen überprüfen, bewerten und testen IKT-Sicherheitsmaßnahmen unter Berücksichtigung des Gesamtrisikoprofils der IKT-Assets des Finanzunternehmens.

(3) Die in Absatz 1 genannten Finanzunternehmen überwachen und evaluieren die Ergebnisse der Sicherheitstests und bringen ihre Sicherheitsmaßnahmen im Falle von IKT-Systemen zur Unterstützung kritischer oder wichtiger Funktionen unverzüglich entsprechend auf Stand.

Artikel 37

Beschaffung, Entwicklung und Wartung von IKT-Systemen

Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen konzipieren und implementieren, sofern angemessen, ein Verfahren für die Beschaffung, Entwicklung und Wartung von IKT-Systemen entsprechend einem risikobasierten Ansatz. Dieses Verfahren muss

a) sicherstellen, dass die funktionalen und nichtfunktionalen Anforderungen, insbesondere auch die Anforderungen an die Informationssicherheit, von der betreffenden Unternehmensfunktion klar spezifiziert und genehmigt werden, bevor IKT-Systeme beschafft oder entwickelt werden;

b) sicherstellen, dass IKT-Systeme vor ihrer erstmaligen Nutzung und vor der Einführung von Änderungen an der Produktionsumgebung getestet und genehmigt werden;

c) Maßnahmen zur Minderung des Risikos einer unbeabsichtigten Veränderung oder einer vorsätzlichen Manipulation der IKT-Systeme während der Entwicklung und Implementierung in der Produktionsumgebung vorsehen.

Artikel 38

IKT-Projekt- und -Änderungsmanagement

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen erarbeiten, dokumentieren und implementieren ein IKT-Projektmanagementverfahren und legen die Aufgaben und Zuständigkeiten für dessen Umsetzung fest. Dieses Verfahren erstreckt sich auf alle Phasen der IKT-Projekte von ihrer Einleitung bis zu ihrem Abschluss.

(2) Die in Absatz 1 genannten Finanzunternehmen entwickeln, dokumentieren und implementieren ein Verfahren für das IKT-Änderungsmanagement, um sicherzustellen, dass alle Änderungen an IKT-Systemen auf kontrollierte Weise und mit angemessenen Schutzvorkehrungen aufgezeichnet, getestet, bewertet, genehmigt, implementiert und verifiziert werden, um die digitale operationale Resilienz des Finanzunternehmens zu wahren.

KAPITEL III

Management der IKT-Geschäftsfortführung

Artikel 39

Komponenten des IKT-Geschäftsfortführungsplans

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen erarbeiten ihre IKT-Geschäftsfortführungspläne unter Berücksichtigung der Ergebnisse der Analyse des Risikos und der potenziellen Auswirkungen von schwerwiegenden Betriebsstörungen und von Szenarien, denen ihre IKT-Assets zur Unterstützung kritischer oder wichtiger Funktionen ausgesetzt sein könnten, insbesondere auch dem Szenario eines Cyberangriffs.

(2) Die in Absatz 1 genannten IKT-Geschäftsfortführungspläne müssen

a) vom Leitungsorgan des Finanzunternehmens genehmigt sein;

b) dokumentiert und im Not- oder Krisenfall leicht zugänglich sein;

c) genügend Mittel für ihre Ausführung vorsehen;

d) die geplanten Wiederherstellungsniveaus und Zeitrahmen für die Wiederherstellung und Wiederaufnahme von Funktionen sowie die wichtigsten internen und externen Abhängigkeiten, insbesondere auch IKT-Drittdienstleister, nennen;

e) festlegen, welche Bedingungen zur Aktivierung der IKT-Geschäftsfortführungspläne führen können und welche Maßnahmen zu ergreifen sind, um die Verfügbarkeit, Kontinuität und Wiederherstellung der IKT-Assets der Finanzunternehmen zur Unterstützung kritischer oder wichtiger Funktionen sicherzustellen;

f) die Wiedergewinnungs- und Wiederherstellungsmaßnahmen für kritische oder wichtige Geschäftsfunktionen, unterstützende Prozesse, Informationsassets und deren Interdependenzen ermitteln, um nachteilige Auswirkungen auf das Funktionieren der Finanzunternehmen zu vermeiden;

g) Verfahren und Maßnahmen für die Datensicherung vorsehen, die den Umfang der Daten, die der Sicherung unterliegen, und die Mindesthäufigkeit der Sicherung auf der Grundlage der Kritikalität der diese Daten nutzenden Funktionen festlegen;

h) Alternativen für den Fall erwägen, dass eine Wiederherstellung wegen Kosten, Risiken, Logistik oder unvorhergesehener Umstände kurzfristig nicht durchführbar sein könnte;

i) die Regelungen für die interne und externe Kommunikation, insbesondere auch Eskalationspläne, festlegen;

j) aktualisiert werden, um den Lehren aus Vorfällen, Tests, neuen Risiken und ermittelten Bedrohungen, veränderten Wiederherstellungszielen sowie größeren Veränderungen der Organisation des Finanzunternehmens und der IKT-Assets zur Unterstützung kritischer oder geschäftlicher Funktionen Rechnung zu tragen.

Für die Zwecke von Buchstabe f sehen die dort genannten Maßnahmen die Minderung von Ausfällen kritischer Drittdienstleister vor.

Artikel 40

Testen der Geschäftsfortführungspläne

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen testen ihre in Artikel 39 der vorliegenden Verordnung genannten Geschäftsfortführungspläne, insbesondere auch die dort genannten Szenarien, mindestens einmal jährlich im Hinblick auf die Sicherungs- und Wiedergewinnungsverfahren oder bei jeder größeren Veränderung des Geschäftsfortführungsplans.

(2) Die in Absatz 1 genannten Tests der Geschäftsfortführungspläne müssen zeigen, dass die in jenem Absatz genannten Finanzunternehmen in der Lage sind, die Funktionsfähigkeit ihrer Geschäftstätigkeit aufrechtzuerhalten, bis kritische Vorgänge wiederhergestellt sind, und etwaige Mängel in diesen Plänen zu erkennen.

(3) Die in Absatz 1 genannten Finanzunternehmen müssen die Ergebnisse der Tests der Geschäftsfortführungspläne dokumentieren, und etwaige bei diesen Tests festgestellte Mängel müssen analysiert, behoben und dem Leitungsorgan gemeldet werden.

KAPITEL IV

Bericht über die Überprüfung des vereinfachten IKT-Risikomanagementrahmens

Artikel 41

Format und Inhalt des Berichts über die Überprüfung des vereinfachten IKT-Risikomanagementrahmens

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen legen den in Absatz 2 jenes Artikels genannten Bericht über die Überprüfung des IKT-Risikomanagementrahmens in einem durchsuchbaren elektronischen Format vor.

(2) Der in Absatz 1 genannte Bericht muss alle folgenden Informationen enthalten:

a) einen einleitenden Abschnitt, der Folgendes enthält:

   i) eine Beschreibung des Kontexts des Berichts mit Blick auf Art, Umfang und Komplexität der Dienstleistungen, Tätigkeiten und Geschäfte des Finanzunternehmens, die Organisation, die ermittelten kritischen Funktionen, die Strategie, die wichtigsten laufenden Projekte oder Tätigkeiten und die Beziehungen des Finanzunternehmens sowie die Abhängigkeit des Finanzunternehmens von internen und ausgelagerten IKT-Dienstleistungen und -Systemen oder die Auswirkungen, die ein Totalverlust oder eine schwerwiegende Verschlechterung derartiger Systeme hinsichtlich kritischer oder wichtiger Funktionen und der Markteffizienz hätte;

   ii) eine Kurzzusammenfassung des ermittelten aktuellen und auf kurze Sicht bestehenden IKT-Risikoprofils, der Bedrohungslage, der erachteten Wirksamkeit seiner Kontrollen und der Sicherheitslage des Finanzunternehmens;

   iii) Informationen über das Gebiet, über das Bericht erstattet wird;

   iv) eine Zusammenfassung der wichtigsten Veränderungen des IKT-Risikomanagementrahmens seit dem letzten Bericht;

   v) eine Zusammenfassung und eine Beschreibung der Auswirkungen der wichtigsten Veränderungen des IKT-Risikomanagementrahmens seit dem letzten Bericht;

b) das Datum der Genehmigung des Berichts durch das Leitungsorgan des Finanzunternehmens, sofern anwendbar;

c) eine Beschreibung der Gründe für die Überprüfung, insbesondere auch,

   i) falls die Überprüfung nach aufsichtsrechtlichen Anweisungen eingeleitet wurde: Belege für diese Anweisungen;

   ii) falls die Überprüfung nach Auftreten von IKT-bezogenen Vorfällen eingeleitet wurde: die Liste aller IKT-bezogenen Vorfälle mit zugehöriger Ursachenanalyse;

d) das Anfangs- und Enddatum des Überprüfungszeitraums;

e) die für die Überprüfung zuständige Person;

f) eine Zusammenfassung der Ergebnisse und eine Eigenbewertung der Schwere der Schwächen, Mängel und Lücken, die im IKT-Risikomanagementrahmen für den Überprüfungszeitraum festgestellt wurden, einschließlich einer detaillierten Analyse derselben;

g) ermittelte Abhilfemaßnahmen zur Behebung von Schwächen, Mängeln und Lücken im vereinfachten IKT-Risikomanagementrahmen und voraussichtliches Datum für die Implementierung dieser Maßnahmen, einschließlich Folgemaßnahmen für in früheren Berichten festgestellte Schwächen, Mängel und Lücken, sofern diese Schwächen, Mängel und Lücken noch nicht behoben sind;

h) allgemeine Schlussfolgerungen zur Überprüfung des vereinfachten IKT-Risikomanagementrahmens, einschließlich weiterer geplanter Entwicklungen.

TITEL IV

SCHLUSSBESTIMMUNGEN

Artikel 42

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 13. März 2024

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN